09/554419 9131

2131

REC'D 20 NOV 2000
WIPO PCT

15

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference PA1065PCT	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/US99/24142	International filing date *(day/month/year)* 14 OCTOBER 1999	Priority date *(day/month/year)* 14 OCTOBER 1998
International Patent Classification (IPC) or national classification and IPC IPC(7): H04L009/00 and US Cl.: 713/201		
Applicant ULTRA INFORMATION SYSTEMS LLC		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 4 sheets.

   ☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority. (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 0 sheets.

3. This report contains indications relating to the following items:

   I ☒ Basis of the report

   II ☐ Priority

   III ☐ Non-establishment of report with regard to novelty, inventive step or industrial applicability

   IV ☐ Lack of unity of invention

   V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

   VI ☐ Certain documents cited

   VII ☐ Certain defects in the international application

   VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
10 MAY 2000	20 JULY 2000
Name and mailing address of the IPEA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer James R. Matthews ROBERT BEAUSOLIEL Telephone No. (703) 308-6107

Form PCT/IPEA/409 (cover sheet) (July 1998)*

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/US99/24142

I. Basis of the report

1. With regard to the **elements** of the international application:*

[X] the international application as originally filed

[X] the description:
pages 1-12 , as originally filed
pages NONE , filed with the demand
pages NONE , filed with the letter of _____

[X] the claims:
pages 13-16 , as originally filed
pages NONE , as amended (together with any statement) under Article 19
pages NONE , filed with the demand
pages NONE , filed with the letter of _____

[X] the drawings:
pages 1-6 , as originally filed
pages NONE , filed with the demand
pages NONE , filed with the letter of _____

[X] the sequence listing part of the description:
pages NONE , as originally filed
pages NONE , filed with the demand
pages NONE , filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

[ ] the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).

[ ] the language of publication of the international application (under Rule 48.3(b)).

[ ] the language of the translation furnished for the purposes of international preliminary examination (under Rules 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

[ ] contained in the international application in printed form.

[ ] filed together with the international application in computer readable form.

[ ] furnished subsequently to this Authority in written form.

[ ] furnished subsequently to this Authority in computer readable form.

[ ] The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

[ ] The statement that the information recorded in computer readable form is identical to the writen sequence listing has been furnished.

4. [X] The amendments have resulted in the cancellation of:

[X] the description, pages NONE

[X] the claims, Nos. NONE

[X] the drawings, sheets/~~fig~~ NONE

5. [X] This report has been drawn as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

** Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17).*

*** Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/US99/24142

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. statement

Novelty (N)	Claims	2-5, 7-10, 12-14	YES
	Claims	1, 6, 11	NO
Inventive Step (IS)	Claims	NONE	YES
	Claims	1-14	NO
Industrial Applicability (IA)	Claims	1-14	YES
	Claims	NONE	NO

2. citations and explanations (Rule 70.7)

Claims 1, 6, and 11 lack novelty under PCT Article 33(2) as being anticipated by WOBBER et al. WOBBER teaches a system in which shared key encryption is used to communicate data securely between computers (col. 2, line 67 to col. 3, lines 62; col. 5 lines 21-34; col. 6, lines 40-62).

Claims 1, 6, and 11 lack novelty under PCT Article 33(2) as being anticipated by LENNON et al. LENNON teaches a communication system in which communicated data in encrypted and decrypted using a common operational key (col. 19, lines 44-62; col. 24, lines 23-37).

Claims 1, 6, and 11 lack novelty under PCT Article 33(2) as being anticipated by DIFFIE et al. DIFFIE teaches a communication system in which data privacy is enforced by the use of shared key cryptography (col. 5, line 60 to col. 6, line 39).

Claim 3 lacks an inventive step under PCT Article 33(3) as being obvious over WOBBER et al. It would have been obvious to one of ordinary skill in the art at the time the invention was made that symmetric key encryption and decryption could have been used to advantage in the WOBBER invention, because these methods would have been widely known to those skilled in the data security art to be effective in securing data.

Claims 4 and 5 lack an inventive step under PCT Article 33(3) as being obvious over WOBBER et al. It would have been obvious to one of ordinary skill in the art at the time the invention was made that a "web server engine" could have been used to send and receive all types of data, including encrypted data, between client and server nodes in the WOBBER invention, because web servers were in common use in many network systems.

Claims 2, 7, and 12 lack an inventive step under PCT Article 33(3) as being obvious over WOBBER et al. in view of LINEHAN et al. WOBBER teaches a shared key encryption system used to communicate data between systems. WOBBER does not explicitly teach that data stored on a server system is encrypted with a (Continued on Supplemental Sheet.)

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: Boxes I - VIII

I. BASIS OF REPORT:

5. (Some) amendments are considered to go beyond the disclosure as filed:
NONE

V. 2. REASONED STATEMENTS - CITATIONS AND EXPLANATIONS (Continued):
private server key. LINEHAN teaches a system in which personal keys are used to encrypt the server data files of different clients in order to provide increased data security (col. 7, lines 39-64). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of LINEHAN with the teachings of WOBBER because a combined system would have had improved data security.

Claims 8 and 13 lack an inventive step under PCT Article 33(3) as being obvious over the prior art as applied in the immediately preceding paragraph and further in view of ROSS, Jr. The WOBBER/LINEHAN combination does not explicitly teach that data is encrypted with a second user's key before data is sent to a second user. ROSS teaches a cryptographic communications system in which data to be communicated to a client system is encrypted with that client's private key before the data is transmitted (col. 2, line 31 to col.3, line 23). It would have been obvious to one of ordinary skill in the art at the time the invention was made that the teachings of ROSS could have been advantageously combined with the teachings of WOBBER and LINEHAN, thus allowing the WOBBER/LINEHAN system to function with increased security.

Claim 9 lacks an inventive step under PCT Article 33(3) as being obvious over the prior art as applied in the immediately preceding paragraph. The WOBBER/LINEHAN/ROSS combination does not explicitly teach that encrypted data sent to a second user can only be viewed on a computer screen by the second user. It would have been obvious to one of ordinary skill in the art at the time the invention was made that only a user who possessed the second user's private key can view data encrypted by that key.

Claims 10 and 14 lack an inventive step under PCT Article 33(3) as being obvious over WOBBER et al. WOBBER does not explicitly teach that data is processed according to user instructions. It would have been obvious to one of ordinary skill in the art at the time the invention was made that server systems are general purpose computers that could be programmed to perform individual actions based on client requests, and that this would increase the usefulness and flexibility of the server system to clients.

---------- NEW CITATIONS ----------
US 4,193,131 A (LENNON et al.) 11 MARCH 1980.
US 5,235,642 A (WOBBER et al.) 11 AUGUST 1993
US 5,812,671 A (ROSS, Jr.) 22 SEPTEMBER 1998
US 5,371,794 A (DIFFIE et al.) 06 DECEMBER 1994
US 5,495,533 A (LINEHAN et al.) 27 FEBRUARY 1996

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/00 — A1

(11) International Publication Number: WO 00/22773

(43) International Publication Date: 20 April 2000 (20.04.00)

(21) International Application Number: PCT/US99/24142

(22) International Filing Date: 14 October 1999 (14.10.99)

(30) Priority Data:
60/104,270 14 October 1998 (14.10.98) US

(71) Applicant *(for all designated States except US)*: ULTRA INFORMATION SYSTEMS LLC [US/US]; Suite 200, 4984 El Camino Real, Los Altos, CA 94022 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: SPRAGGS, Lynn [CA/CA]; 8604 Kalavista Drive, Vernon, British Columbia V1B 1K3 (CA).

(74) Agents: TOCZYCKI, Robert et al.; Carr & Ferrell LLP, Suite 200, 2225 East Bayshore Road, Palo Alto, CA 94303 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

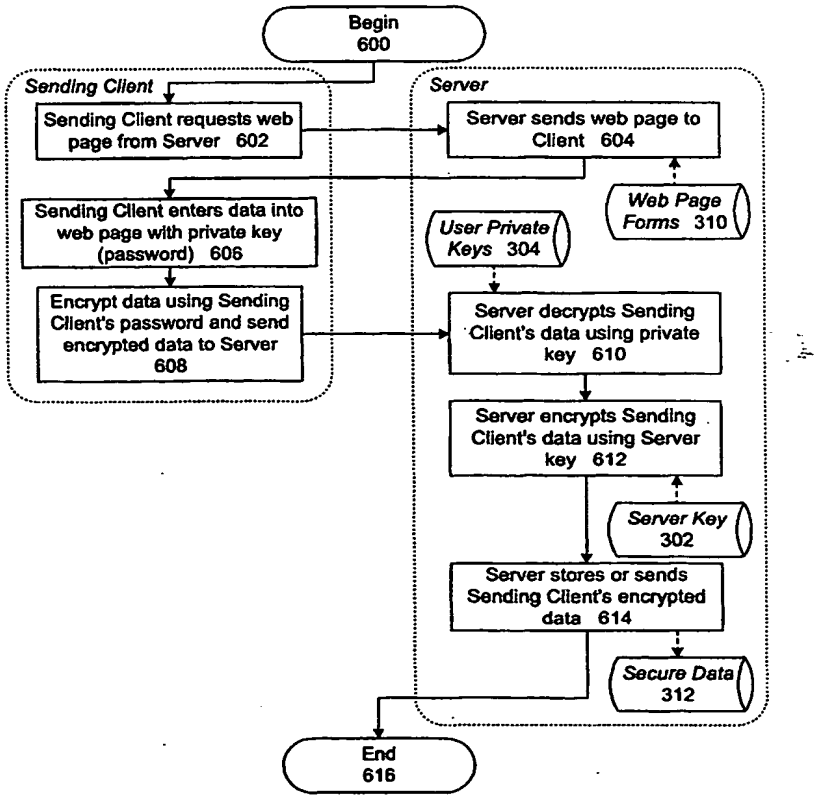
With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: SYSTEM AND METHOD OF SENDING AND RECEIVING SECURE DATA WITH A SHARED KEY

(57) Abstract

A server computer (100) sends and receives secure data provided by authorized users (102, 104). The data is secured by encrypting (608) and decrypting (610) the data with a key that is shared between the users and the server computer. As the server computer receives a user's encrypted data, the server computer decrypts the data using the user's shared key (304) stored in a database on the server. The server computer can then process the data according to the user's instructions, this could include securely storing the data for retrieval by another user (614), processing the data, and/or securely sending the data to a second user by encrypting the data with the user's shared key (708).



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/24142

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) : H04L009/00
US CL : 713/201

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/201; 705/35; 705/65; 380/258; 380/286

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CAS ONLINE; EAST; IEEE

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 4,193,131A (LENNON et al.) 11 March 1980, col 19, line 44 to col. 24, line 20.	1-14
Y	US 5,148,479A (BIRD et al.) 15 September 1992, col. 6, lines 22-58.	1-14
Y	US 5,649,118A (CARLISLE et al.) 15 July 1997, col. 8, lines 10-64	1-14
Y	US 5,544,246A (MANDELBAUM et al.) 6 August 1996, col 6, lines 34-67.	1-14
Y	US 5,724,424A (GIFFORD) 3 March 1998, col. 10, lines 43-53.	1-14

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 JANUARY 2000	16 FEB 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer ROBERT G. CROCKETT Telephone No. (703) 308-6107

Form PCT/ISA/210 (second sheet)(July 1992)★

#25/E
9-20-04
13.0.14

DETAILED ACTION

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. Lynn Spraggs on September 17, 2004.

The application has been amended as follows:

IN THE CLAIMS:

16. (New) A system for using a shared key to transmit secure data between a client and a server, the system comprising:

an encrypt/decrypt engine for using the shared key to encrypt or decrypt data, the encrypt/decrypt engine being configured for delivery via a web page to a client in response to a user request and further configured to encrypt data independently of an identity of the physical client;

wherein the server includes a user private keys database configured to store the shared key, [[.]] ~~And,~~ and wherein, it is possible for the client and the server to reside on the same physical computing device, [[.]] ~~And when~~ and where the shared key is

derived from the user's authentication data, and the derived shared key is used for encrypting all data.

16. (Previously) The system of claim 15 wherein the shared key is a user's private key entered by a user into the web page.

17. (Previously) The system of claim 15 further comprising a secure data database configured to store data received from the client and, upon the completion of a processing step, to deliver the stored data in an encrypted format to the client or to another client.

18. (Previously) The system of claim 15 further comprising a secure data database configured to store data received from the client and, upon receipt of a request for the data, to deliver the stored data in an encrypted format to the client or to another client.

19. (New) The system of claim 15 wherein the shared key is transmitted between the server and the client as few as zero times and the shared key is transmitted between the server and the user as few as one time, [[.]] ~~The,~~ the key is not sent for authentication purposes, rather, the effect of the key in the encryption process is sent, [[.]] ~~Consequently,~~ consequently, the shared key does not need to be retransmitted once it has been established.

20. (Previously) The system of claim 15 wherein the shared key is a user's private key entered by a user.

21. (Previously) The system of claim 15 wherein the client encrypt/decrypt engine is installed on the client.

8 22. (New) A system for using a shared key in transmitting secure data between a client and a server, the system comprising:

an encrypt/decrypt engine for using, the shared key, in encrypting data, the encrypt/decrypt engine being configured to encrypt data independently of an identity of the client;

and a user private keys database located on the server and configured to store the shared key, the shared key being the private key of a user, [[.]] ~~And when~~ and where the shared key is derived from the user's authentication data, and the derived shared key is used for encrypting all data.

E' 9 23. (New) The system .of claim 22 wherein the server is configured to decrypt encrypted data received from the client using the shared key and to use a private server key, known only by the server, to re-encrypt the decrypted data.

10 24. (New) The system of claim 23 further comprising a secure data database configured to store the encrypted data received from the client and re-encrypted by the server and to deliver the stored data to the client or to another client; the delivered data, after the completion of a processing step, being encrypted with the shared user key or with another shared user key, [[.]] ~~And when~~ and where the shared key is derived from the user's authentication data, and the derived shared key is used for encrypting all data.

11 25. (New) The system of claim 23 further comprising a secure data database configured to store the encrypted data received from the client and re-encrypted by the server and to deliver the stored data to the client or to another client; the delivered data being, upon receipt of a request for the data, encrypted with the shared user key or with another

shared user key, where the shared key is derived from the user's authentication data, and the derived shared key is used for encrypting all data.

26. (Previously) The system of claim 25 wherein the request is from the user.

27. (Previously) The system of claim 25 wherein the request is from an other user.

28. (New) A system for using a shared key in transmitting secure data between a client and a server, the system comprising:

an encrypt/decrypt engine for using the shared key entered by a user to encrypt data entered by the user, the encrypt/decrypt engine being configured such that all data entered by the user and stored on the client is stored in encrypted form, and further configured to encrypt data independently of an identity of the physical client; the shared key entry being the responsibility of the user and not the client; the server including a user private keys database configured to store the shared key, the shared key being a private key of a user; and not a physical client and, ~~when~~ where the shared key is derived from the user's authentication data and the derived shared key is used for encrypting all data.

29. (Previously) The system of claim 28, wherein the encrypt/decrypt engine uses a symmetric key encryption/decryption algorithm for encrypting and decrypting data.

30. (Previously) The system of claim 28, further including a web server engine configured for the user to securely send or receive data from the client to the server.

31. (New) A method for using a shared key in receiving secure data on a server, comprising the steps of:

delivering from a server to a client a web page including an encrypt/decrypt engine; encrypting data on the client using the encrypt/decrypt engine and a shared key entered by a user of the client, the shared key being shared between the user aid the server;

delivering the encrypted data from the client to the server; ~~when~~ where the shared key is derived from the user's authentication data and the derived shared key is used for encrypting all data; receiving the encrypted data at the server; decrypting the encrypted data at the server using the shared

key; and processing the decrypted data, ~~when~~ where the shared key is derived from the user's authentication data and the derived shared key is used for encrypting all data.

32. (Previously) The method of claim 31, wherein the step of processing the decrypted data includes the steps of: encrypting the decrypted data with a private server key; and storing the encrypted data in a database.

33. (Previously) The method of claim 31, wherein the step of processing the decrypted data includes the steps of: re-encrypting the data with an other user's private key shared between the other user and the server; and sending the re-encrypted data to the other user.

34. (Previously) The method of claim 31, wherein the step of processing the decrypted data includes the steps of: decrypting the encrypted data with the private server key; re-encrypting the data with a second user's key shared between the second user and the server; and sending the re-encrypted data to the second user.

21 35. (Previously) The method of claim 31, wherein the step of processing the decrypted data includes the steps of: processing the data according to an instruction of the user; re-encrypting the processed data using the user's shared key; and sending the re-encrypted processed data to the user.

22 36. (Previously) The method of claim 31, wherein the step of, processing the decrypted data includes storing the decrypted data in a secure database.

23 37. (New) A computer-readable medium comprising program instructions for causing a computer system to use a shared key in receiving secure data at a server, by the steps of:

delivering a web page from the server to a client, the web page including an encrypt/decrypt engine and being configured to use the encrypt/decrypt engine and a shared key entered by a user of the client to encrypt data on the client; the shared key being shared between the user and the server; receiving the encrypted data at then server; decrypting the encrypted data using the shared key; and processing the decrypted data ~~and when~~ where the shared key is derived from the user's authentication data and the derived shared key is used for encrypting all data.

24 38. (New) A computer-readable medium comprising program instructions for causing a computer system to receive secure data on a server using a shared key, by the steps of: delivering an encrypt/ decrypt engine from the server to a client, the encrypt/decrypt engine being configured to use a shared key entered by a user of the client to encrypt data on the client, the shared key being shared between the user and the server and the encryption being independent of an identity of the physical client; receiving the

encrypted data at the server; decrypting the encrypted data using the shared key; and processing the decrypted data, ~~when~~ where the shared key is derived from the user's authentication data and the derived shared key is used for encrypting all data.

25 39. (Previously) The computer readable medium of claim 38, 24 further comprising program instructions for causing the processed decrypted data to be re-encrypted using a private server key.

26 40. (Previously) The computer-readable medium of claim 39, 25 further comprising program instructions for causing the processed decrypted data to be stored in a secure database.

27 41. (Previously) The computer-readable medium of claim 38, 24 wherein processing the decrypted data includes the steps of: re-encrypting the data with the private server key; storing the re-encrypted data; decrypting the stored data with the private server key; encrypting the data with a second user's key shaved between the second user and the server; and sending the encrypted data to the second user.

28 42. (Previously) The computer-readable medium of claim 38 24 wherein processing the decrypted data includes the steps of: processing the data according to an instruction of the user; encrypting the processed data using a shared key; and sending the encrypted processed data to the user or to another user.

29 43. (New) A method of using a shared key in transmitting secure data between a client and a server using a shared key, comprising the steps of: encrypting data using the shared key with an encrypt/decrypt engine configured to encrypt data independently of an identity of the client, the shared key being entered by a user of the client; delivering

the encrypted data from the client to the server; receiving the encrypted data at the server; decrypting the encrypted data, at the server using the shared key, the shared key being stored in a user private keys database; and processing the decrypted data, ~~when~~ where the shared key is derived from the user's authentication data and the derived shared key is used for encrypting all data.

30 44. (Previously) The method of claim 43, 29 wherein processing the decrypted data includes the steps of: encrypting the decrypted data with a private server key; and storing the encrypted data, in a database.

31 45. (Previously) The method of claim 43, 29 wherein the step of processing the decrypted data includes the steps of: encrypting the data with an other user's private key shared between the other user and the server; and sending the encrypted data to the other user.

32 46. (Previously) The method of claim 43, 29 wherein the step of processing the decrypted data includes the steps of: decrypting the re-encrypted data with the private server key; encrypting the data with a second user's key shared between the second user and the server; and sending the encrypted data to the second user.

33 47. (Previously) The method of claim 43, 29 wherein the step of processing the decrypted data includes the steps of: processing the data according to an instruction of the user; re-encrypting the processed data using the user's shared key; and sending the re-encrypted processed data to the user.

Allowable Subject Matter

The following is an examiner's statement of reasons for allowance: The present invention is directed to a system for secure transfer of data between a client and a server. Each independent claim identifies the uniquely distinct feature "of an encrypt/decrypt engine using a key shared between the client and server where the shared key is derived from the user's authentication data and the derived shared key is used for encrypting all data" The prior art, Laursen et al (US 6,065,120) discloses a conventional security system between a client and server, either singularly or in combination, fails to anticipate or render the claimed limitation obvious.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B Smithers whose telephone number is (703) 308-9293. The examiner can normally be reached on Monday-Friday (9:00-5:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew T Caldwell can be reached on (703) 306-3036. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Matthew B Smithers
Primary Examiner
Art Unit 2137